UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ANDRE LOPEZ, on behalf of himself and all others similarly situated,

Plaintiff,

v.

TEACHERS INSURANCE AND ANNUITY ASSOCIATION OF AMERICA,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Andre Lopez ("Plaintiff"), on behalf of himself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against the above-captioned Defendant, Teachers Insurance and Annuity Association of America ("TIAA") (the "Defendant") upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of counsel as follows:

I. NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against Defendant TIAA for its failure to properly secure and safeguard personally identifiable information ("PII") including but not limited to: Plaintiff's and Class members' name, Social Security number, gender, date of birth, and physical address.

2. Defendant is a substantial financial services corporation with the resources to take seriously the obligation to protect private information. However, TIAA failed to invest the time or resources necessary to protect the PII of Plaintiff and Class members.

3. Defendant TIAA is a New York based financial services organization that provides services (such as retirement and annuity-related services) to academic, research, medical, cultural, and governmental employees. With over $1 trillion in assets under management, TIAA has been ranked as one of the 500 largest corporations in the United States.

4. Defendant TIAA hired an entity called PBI, a vendor that provides search tools to financial services institutions such as TIAA. PBI, in turn, hired PSC, a software company, for the storage and transfer of TIAA's client data entrusted to PBI. PBI uses PSC's MOVEit transfer file services for a variety of purposes, including the transfer of Plaintiff's and Class members' PII. Like millions of Americans, Plaintiff's and the Class members' PII was given to TIAA for financial

purposes and was entrusted by TIAA to PBI. In undertaking this responsibility, TIAA and PBI were both obligated to only hire vendors who maintain adequate data security practices and PSC is obligated to ensure than their file transfer systems – like MOVEit – are secure. However, due to a significant and troubling vulnerability in PSC's MOVEit software, the PII entrusted by TIAA to PBI by over 2,300,000 retirees, pension holders, and other financial customers was compromised.

5. According to the Notice of Data Breach received by Plaintiff, which was received not from Defendant TIAA but from a third-party, PBI, on or around May 31, 2023, PSC's MOVEit software disclosed a major vulnerability that was exploited by an unauthorized cybercriminal. Over the course of investigating, PBI, who uses PSC in order to transfer files of TIAA's clients using the MOVEit software system, discovered that, between May 29, 2023 and May 30, 2023, third-party cybercriminals not only exploited the MOVEit software, but downloaded and exported the data of Plaintiff and Class members (the "Data Breach"). This Data Breach was likely perpetrated by a well-known cybergang called Clop. The *modus operandi* of a cybergang like Clop is to offer for sale (on the dark web) unencrypted, unredacted private information like the PII of Plaintiff and the Class members. Thus, the Plaintiff and Class members are in imminent harm of identity theft and other identity-related crimes.

6. To compound matters, Defendant's conduct following the Data Breach has been woefully insufficient: (1) TIAA never even informed Plaintiff directly of the harm he suffered due to the Data Breach; (2) third-party PBI did not disclose the Data Breach to victims until July 14, 2023 – nearly six weeks after the Data Breach was first discovered on May 31, 2023; (3) the Notice of Data Breach failed to disclose the specifics of the cyberattack (*i.e.*, how it happened) as well as specific remedial measures taken to ensure the protection of the PII still in Defendant's possession;

and (4) the only remediation here was not even offered by TIAA, it was offered by PBI: a meager 24 months of identity theft protection for victims of the Data Breach when the impact of the theft of this sort of PII set at-issue will ripple for many years, if not decades. By continuing to drag its feet, Defendant allowed cybercriminals to get a running start on harms to Plaintiff and the Class members, rather than accepting responsibility for Defendant's failures within their data storage, data systems and relevant cybersecurity apparatus. While Defendant could have given Plaintiff and the Class members the ability to start acting (like imposing credit freezes) to protect themselves, Defendant continues to make a conscious decision not to do so.

7. Notably, the Data Breach response was worsened too by the fact that PBI was the issuer of the Notice of Data Breach – a third-party that most Class members have never heard of. Undoubtedly, this led to Class members discarding the Notice of Data Breach. Hence, to this day, those Class members have no knowledge that they are even victims. TIAA should have been the entity responsible for the distribution of said notices, as Class members all had accounts with TIAA and might have had a better chance of being responsive to an entity they are familiar with.

8. Upon information and belief, TIAA negligently chose to utilize PBI's search services with Plaintiff's and Class members' PII even though the MOVEit software contained significant security vulnerabilities. The mechanism and potential for this Data Breach was a known risk to Defendant because of other file transfer programs that had been previous subjected to criminal hacking, and, thus, Defendant were on notice that failing to take appropriate design and protective measures would expose and increase the risk that PII would be compromised and stolen.

9. As such, Plaintiff, on behalf of himself and all others similarly situated, brings this Action for restitution, actual damages, nominal damages, statutory damages, injunctive relief, disgorgement of profits and all other relief that this Court deems just and proper.

II. JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount of controversy exceeds the sum of $5,000,000 exclusive of interests and costs, there are more than 100 putative Class members, and minimal diversity exists because one or more putative Class members are citizens of a different state than Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in New York, New York. Furthermore, Defendant intentionally availed itself of this jurisdiction by marketing, employing individuals, and providing financial services in New York, New York.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant operates in this District and a substantial part of the events, acts and omissions giving rise to Plaintiff's claims occurred in this District.

III. PARTIES

Plaintiff Andre Lopez

13. Plaintiff Andre Lopez is, and at all times mentioned herein, was an individual citizen of the state of New Jersey. Plaintiff Lopez was employed by an organization that, upon information and belief, gave his PII to TIAA in order to administer a 401k retirement plan of which Plaintiff Lopez was a beneficiary. Plaintiff Lopez received a copy of the Notice of Data Breach disseminated by PBI.

14. As a result of Defendant's failure to protect Plaintiff Lopez's PII, Plaintiff Lopez's PII has been compromised in the Data Breach.

Defendant TIAA

15. Defendant Teachers Insurance and Annuity Association of America is domiciled and maintains its principal place of business in the State of New York.

16. TIAA offers financial services to over five million people and manages over $1 trillion in assets under management.

17. According to the Notice of Data Breach, TIAA hired PBI. PBI is a third-party vendor which offers search services to pension funds, insurance companies, and others, like TIAA, to determine various data points, such as whether a fund recipient is deceased. PBI uses MOVEit file transfer for these purposes, amongst others, including the transfer and/or storage of Plaintiff's and Class members' PII. MOVEit file transfer is a product of PSC. PSC is a third-party software vendor that offers a wide range of products and services to government agencies and corporate entities around the world, including MOVEit. MOVEit is a "[m]anaged file transfer and automatic software that guarantees the security of sensitive files both at-risk and in-transit, ensures reliable business processes and addresses data security compliance requirements."

IV. FACTUAL ALLEGATIONS

Defendant's Businesses and Collection of Private Information

18. In the course of doing business, TIAA acquires a significant amount of highly valuable private information from its' financial services consumers, including the acquisition of the PII of Plaintiff and the Class members.

19. According to the Notice of Data Breach, TIAA hired PBI to provide various search-related functions that were necessary to carry out TIAA's business. In the process of doing this,

PBI acquired a significant amount of TIAA consumers' private information, including the PII of Plaintiff and the Class members. To store and transfer said PII, PBI hired PSC to use PSC's MOVEit file storage and transfer system.

20. As a condition of receiving the PII, Plaintiff and Class members entrusted that TIAA would only use their data for business purposes in a way that was safe and secure, and that includes and extends to the hiring of any third party contracted to provide services on behalf of TIAA.

21. TIAA makes cybersecurity promises with respect to the data it collects. For example, TIAA, states that "[t]he privacy of your personal information is something [TIAA takes] seriously." TIAA makes promises to keep data secure, but, at no point does TIAA state that it would willingly give over Plaintiff's and Class members' PII to third-party vendors who would not keep their PII safe.

22. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for ensuring the security and safety of Plaintiff and Class members' PII to protect it from unauthorized disclosure and exfiltration.

23. Plaintiff and the Class members relied on Defendant to keep their PII confidential and security maintained, and only to make authorized disclosures of this information, which Defendant failed to do.

The Data Breach

24. On May 31, 2023, PSC reported a vulnerability in MOVEit Transfer and MOVEit Cloud that could lead to escalated privileges and potential unauthorized access to the data

environment. PSC purportedly launched an investigation, alerted MOVEit customers of the issue and provided mitigation steps.

25. This was confirmed by PBI in their Notice of Data Breach received by the Plaintiff. According to the Notice of Data Breach:

> **What Happened?** On or around May 31, 2023, [PSC], the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, [PBI] learned that the third party accessed one or more of MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data.
>
> …
>
> **What Information Was Involved?** [PBI's] investigation determined that the following types of information related to [victim] were present in the server at the time of the event: name, Social Security number, gender, date of birth, and address.

26. Not only do the Class members have to contend with the harm that the Data Breach caused, but Defendant's individual response has been woefully insufficient.

27. First, Defendant – to this day – has not informed Plaintiff about the Data Breach. In fact, no one disclosed this Data Breach to victims until July 14, 2023, six weeks after Defendant first became aware of it. That means that, for nearly six weeks, Defendant could have alerted victims to the fact that their PII was compromised but failed to do so. Instead, Defendant chose to sit on that information and allow valuable time to pass while Plaintiff and members of the Class suffered the harms discussed herein.

28. Second, TIAA has offered the victims nothing. Only third-party vendor PBI has Defendant offered victims an insufficient 24 months of identity theft monitoring services when the impact of the theft of the PII at-issue ripples for decades. Although it is well-documented that the

harms from identity theft can affect a person for a lifetime, Defendant refuses to provide the victims of the Data Breach with adequate protection.

29. Finally, the disclosure itself was inadequate. The Notice of Data Breach did not disclose the specifics of the cyberattack as well as the specific remedial measures being taken to ensure the protection of the PII still in Defendant's and the third-party vendors' possession. All of this information remains unclear to the victims of the Data Breach.

30. What is clear, however, is that cybercriminals did download and exfiltrate the PII of Plaintiff and the Class members. As such, Defendant did not implement or maintain adequate measures to protect its victims PII from attackers and cyber criminals.

31. On information and belief, the PII compromised in the files accessed by hackers was not encrypted. This can also be inferred given that Clop was able to access the data that was listed as compromised in the Notice of Data Breach.

32. Moreover, the removal of PII from Defendant's systems demonstrates that this cyberattack was targeted by Clop due to Defendant's status as a premier financial services facility that houses sensitive PII. And, armed with this PII, data thieves, like Clop (as well as downstream purchasers of the stolen PII), can commit a variety of crimes, including: opening new financial accounts in Class members' names, taking out loans in Class members' names, using Class members' information to obtain government benefits, filing fraudulent tax returns using Class members' tax identification information, obtaining driver's licenses in Class members' names but with a different photograph, and giving false information to police during an arrest.

33. Due to Defendant's flawed security measures, flawed oversight of third-party vendors and incompetent response to the Data Breach, Plaintiff and the Class members now face

a present, substantial, and imminent risk of fraud and identity theft and must deal with that threat forever.

34. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII, and despite Defendant's generous operating budget, Defendant provided unreasonably deficient protections prior to the Data Breach, including but not limited to a lack of security measures for storing and handling PII, as well as inadequate employee training regarding how to access, oversee the protection, handle and safeguard for this sensitive set of information.

35. Defendant failed to adequately adopt and train its employees and third-parties on even the most basic of information security protocols, including storing, locking, encrypting and limiting access to current and former consumers and employees' highly sensitive PII; implementing guidelines for accessing, maintaining, and communicating sensitive PII; and protecting sensitive PII by implementing protocols on how to utilize such information.

36. Defendant's failures caused the unpermitted disclosure of Plaintiff's and Class members' PII to an unauthorized third-party cybercriminal and put Plaintiff and Class members at serious, immediate, and continuous risk of identity theft and fraud.

37. The Data Breach that exposed Plaintiff's and Class members' PII was caused by Defendant's violation of its obligations to abide by best practices and industry standards concerning its information security practices and processes.

38. Defendant, despite being a technologically advanced organization, failed to comply with basic security standards or to implement security measures that could have prevented or mitigated the Data Breach.

39. Defendant failed to ensure that all personnel (and third-parties) with access to its current/former consumers' PII were properly trained in retrieving, handling, using and distributing sensitive information. Further, there have been no assurances offered by Defendant that all personal data or copies of the PII at issue were either recovered, destroyed, or otherwise protected by an enhanced data security protection apparatus.

The Breach Was Foreseeable

40. Defendant has weighty obligations created by industry standards, common law, and its own promises and representations to keep PII confidential and to protect it from unauthorized access and disclosure.

41. Plaintiff and Class members provided their PII to TIAA with the reasonable expectation and mutual understanding that TIAA would comply with its obligations to keep such information confidential and secure from unauthorized access. This expectation and mutual understanding extended to third party vendors that TIAA uses for business purposes.

42. Defendant's data security obligations were particularly acute given the substantial increase in ransomware attacks and/or data breaches in various industries (especially including the financial services industry) preceding the date of the Data Breach.

43. Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

44. Cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

45. PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners. PII can be used to distinguish,

identify or trace an individual's identity. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as the information compromised in the Data Breach.

46. Given the nature of the Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of different ways.

47. Cybercriminals who possess the Class members' PII can readily obtain Class members' tax returns or open fraudulent credit card or other types of accounts in the Class members' names.

48. The increase in such attacks, and attendant risk of future attacks, was widely known.

49. As such, this specific Data Breach was foreseeable. Defendant was cognizant of data breaches because of how common and high-profile data breaches have become with respect to consumer-facing businesses such as Defendant, a financial services organization.

Defendant Failed to Follow FTC Guidelines, the Gramm-Leach-Bliley Act and Industry Standards

50. Experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the data which they collect and maintain. The reason this data is so valuable is because it contains PII, which can be sold and weaponized for purposes of committing various identity theft-related crimes. It is well-known that, because of the value of this data and PII, businesses that collect, store, maintain, and otherwise utilize or profit from PII must take necessary cybersecurity safeguards to ensure that the data they possess is adequately protected.

51. Government agencies also highlight the importance of cybersecurity practices. For example, the Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

52. According to the FTC, the need for data security should be factored into all business decision-making.

53. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

54. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

55. The guidelines also recommend that businesses use an intrusion detection system to detect and expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

56. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

57. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, in some cases treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data as

an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further explicate and clarify the measures businesses must take to meet their data security obligations.

58. Defendant failed to properly implement some or all of these (and other) basic data security practices.

59. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

60. Additionally, Defendant provides financial services for consumers and is therefore subject to the Gramm-Leach-Bliley Act ("GLBA"). Defendant collects non-public information as a financial institution and therefore was subject to the requirements of the GBLA, 15 U.S.C. § 6801.1, *et seq.*, as well as the GBLA Privacy Rules and other related regulations. The GBLA requires numerous safeguards to protect private information for which Defendant apparently did not comply, including overseeing service providers and requiring them by contract to protect the security and confidentiality of consumer information.

61. Defendant's failure to oversee PSC and PBI constitutes a violation of GLBA.

62. Defendant was at all times fully aware of its obligation to protect PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

63. Experts studying cyber security routinely identify consumer-facing businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

64. Several best practices have been identified that, at a minimum, should be implemented by financial services providers such as TIAA (and its third party vendors), including

but not limited to: educating all employees about cyber security; requiring strong passwords; maintaining multi-layer security, including firewalls, anti-virus, and anti-malware software; utilizing encryption; making data unreadable without a key; implementing multi-factor authentication; backing up data; and limiting which particular employees can access sensitive data.

65. Other best cybersecurity practices that are standard in the industry include installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; and training staff regarding critical points.

66. These foregoing frameworks are existing and applicable industry standards. Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant's Breaches of Its Obligations

67. Defendant breached its obligations to Plaintiff and Class members and was otherwise negligent and/or reckless because it failed to properly maintain, oversee and safeguard its computer systems, network and data. In addition to its obligations under federal and state law, Defendant owed a duty to Plaintiff and the Class members to exercise reasonable care when obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including complying with industry standards and requirements, training for its staff and ensuring that their collective computer systems, networks, and protocols adequately protected the PII of Plaintiff and the Class members.

68. Defendant wrongful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect current or former consumers' PII;

c. Failing to properly monitor third-party data security systems for existing intrusions, brute-force attempts and clearing of event logs;

d. Failing to ensure that all third-parties apply all available and necessary security updates;

e. Failing to ensure that all third-parties install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to ensure that all third-parties practice the principle of least-privilege and maintain credential hygiene; and failing to avoid the use of domain-wide, admin-level service accounts;

g. Failing to adequately oversee third-party vendors;

h. Failing to ensure that all third-parties employ or enforce the use of strong randomized, just-in-time local administrator passwords; and

i. Failing to properly train and supervise third-parties in the proper handling of inbound emails.

69. As the result of allowing its computer systems to fall into dire need of security upgrading and its inadequate procedures for handling cybersecurity threats, Defendant negligently and wrongfully failed to safeguard Plaintiff's and Class members' PII.

70. Accordingly, as further detailed herein, Plaintiff and Class members now face a substantial, increased, and immediate risk of fraud, identity theft, and the disclosure of their most sensitive and deeply personal information.

Data Breaches are Disruptive and Harm Victims

71. The United States Government Accountability Office ("GAO") released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

72. That is because all victims of a data breach may be exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it because there is (unfortunately) a market for personally identifiable information, like the PII compromised by the Data Breach.

73. Cybercriminals do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate individual pieces of data an identity thief obtains regarding a person, the easier it is for that thief to take on the victim's identity, or otherwise harass or track the victim.

74. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information regarding a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

75. The type of information compromised in this Data Breach is even worse than merely a name and date of birth. A stolen Social Security number is a skeleton key to the victim's identity – and, therefore, the type of data that cyberthieves seek. Identity thieves can use a Social Security number for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, fraudulently obtaining a job, fraudulently renting a house, or filing a false police report.

76. Because of the threat of these harms, the FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and potentially obtaining an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

77. Theft of PII is gravely serious. PII is an extremely valuable property right.

78. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates that PII has considerable market value.

79. According to the GAO:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

80. Private information, such as the PII compromised herein, is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. The private information of consumers

remains of high value to criminals, as evidenced by the prices paid through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, private information (inclusive of a Social Security number) can be sold at a price from $40 to $200, and bank details have a price range of $50 to $200. Experian reports that a stolen credit card or debit card number can sell between $5 to $110 on the dark web. Clearly, all this data has real value – which is why it was targeted and stolen in the first place.

81. Because of the value of the PII compromised in the Data Breach, there is a strong probability that entire batches of information stolen in the Data Breach have been dumped on the black market, as that is the *modus operandi* of cybercriminals who perpetrate data breaches, while other batches have yet to be dumped on the black market, meaning Plaintiff and Class members are at a substantial imminent risk of injury including an increased risk of fraud and identity theft for many years into the future.

82. Thus, Plaintiff and Class members must vigilantly monitor their financial accounts and other indices of identity theft (*i.e.*, the mail, email, etc.) for many years to come.

Harm to Plaintiff and the Class

83. On or about July 14, 2023, Plaintiff received notice from PBI that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff's PII was compromised as a result of the Data Breach. Plaintiff still has not heard from TIAA about the Data Breach.

84. As a result of being informed about the Data Breach (by a third-party), Plaintiff has commenced making reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing reports and his financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff has already

spent multiple hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

85. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) actual misuse of his compromised PII; (b) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff; (c) violation of his privacy, including the compromise of highly sensitive PII such as, for example, his Social Security numbers in combination with name and other private information; (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud; and (e) actual and potential out-of-pocket losses including the loss of time, as Plaintiff has spent multiple hours dealing with the repercussions of the Data Breach, due to time spent mitigating the actual and potential harms caused by the Data Breach.

V. CLASS ALLEGATIONS

86. Plaintiff brings this nationwide class on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure. The "Class" that the Plaintiff seeks to represent is defined as follows:

> **Class Definition.** All persons whose PII was maintained by TIAA and compromised in the Data Breach.

87. Excluded from the Class are Defendant and Defendant's subsidiaries, affiliates, officers and directors, and any entity in which the Defendant has a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

88. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

89. **Numerosity**. Defendant reports to the Maine Attorney General that the Data Breach compromised PII over 2.3 million current consumers. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

90. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost or disclosed Plaintiff's and Class members' PII;

b. Whether Defendant(and its third-party vendors) failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's (and its third-party vendors') data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's(and its third-party vendors') data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Plaintiff and Class members to safeguard their PII;

f. Whether Defendant breached its duty to Plaintiff and Class members to safeguard their PII;

g. Whether computer hackers obtained Plaintiff's and Class members' PII in the Data Breach;

h. Whether Defendant knew or should have known that its (and its third-party vendors') data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's acts, inactions, and practices complained of herein amount to a breach of contract, violations of N.Y. Gen. Bus. Law 349

and/or common law negligence, and whether Defendant has been unjustly enriched;

k. Whether Defendant failed to provide notice of the Data Breach in a timely and proper manner; and

l. Whether Plaintiff and Class members are entitled to damages, civil penalties, punitive damages, equitable relief and/or injunctive relief.

91. **Typicality**. Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiff, like all Class members, was injured by Defendant's uniform conduct. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

92. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Class in that they have no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiff suffered are typical of the other Class members, and Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class. Plaintiff has retained counsel experienced in complex class action litigation, including, but not limited to, data privacy class action litigation, and Plaintiff intends to prosecute this action vigorously.

93. **Superiority of Class Action**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class's common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in

individual actions that are based upon an identical set of facts. Without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

94. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

95. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

96. **Predominance**. The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Defendant has engaged in a common course of conduct toward Plaintiff and Class members. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these issues in a single action has important and desirable advantages of judicial economy.

97. This proposed class action does not present any unique management difficulties.

COUNT I

NEGLIGENCE

98. Plaintiff and the Class repeat and re-allege each and every allegation as if fully set forth herein.

99. Defendant knowingly collected, acquired, stored, and/or maintained Plaintiff's and Class members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and

protecting the PII from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

100. The duty included obligations to take reasonable steps to prevent disclosure of the PII, and to safeguard the information from theft. Defendant's duties included the responsibility to design, implement, and monitor its and its third-party vendors' data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

101. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the PII.

102. Defendant owed a duty of care to safeguard the PII due to the foreseeable risk of a data breach and the severe consequences that would result from its failure to so safeguard the PII.

103. Defendant's duty of care to use (and to ensure that its third-party vendors used) reasonable security measures arose as a result of the special relationship that existed between Defendant and those individuals who entrusted them with their PII, which is recognized by laws and regulations including but not limited the FTC Act, GLBA, as well as common law. Defendant was in a position to ensure that its vendor's systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

104. In addition, Defendant has a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

105. Defendant's duty to use reasonable care in protecting PII arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect PII that it either acquires, maintains, or stores.

106. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII, as alleged and discussed above.

107. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' PII would result in injury to Plaintiff and Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the data transfer and storage industry.

108. It was therefore foreseeable that the failure to adequately safeguard Class members' PII would result in one or more types of injuries to Class members.

109. The imposition of a duty of care on Defendant to safeguard the PII they maintained, transferred, stored or otherwise used is appropriate because any social utility of Defendant's conduct is outweighed by the injuries suffered by Plaintiff and Class members as a result of the Data Breach.

110. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are at a current and ongoing imminent risk of identity theft, and Plaintiff and Class members sustained compensatory damages including: (i) invasion of privacy; (ii) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial "out of pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their PII; (viii) future costs of identity theft

monitoring; (ix) anxiety, annoyance and nuisance, and (x) the continued risk to PII, which remains in Defendant's and the third-party's respective control, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

111. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

112. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and unsecure manner.

113. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

COUNT II

BREACH OF CONTRACT

114. Plaintiff repeats and re-alleges each and every allegation as if fully set forth herein.

115. TIAA entered into contracts with customers, agents, and businesses to provide financial services; services that included data security practices, procedures, and protocols sufficient to safeguard the PII that was entrusted to it.

116. Plaintiff and Class members were parties to such contracts, as it was their PII that TIAA agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties.

117. TIAA knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class members would be harmed.

118. TIAA breached its contracts with customers by, among other things, failing to adequately secure Plaintiff and Class members' PII, and, as a result, Plaintiff and Class members were harmed by TIAA's failure to secure their PII.

119. As a direct and proximate result of TIAA's breach, Plaintiff and Class members are at a current and ongoing risk of identity theft, and Plaintiff and Class members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their PII; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their PII, which remains in TIAA's control, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

120. Plaintiff and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

121. Plaintiff and Class members are also entitled to injunctive relief requiring TIAA to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT III

VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349

122. Plaintiff repeats and re-alleges each and every allegation as if fully set forth herein.

123. New York General Business Law Section 349 ("New York Gen. Bus. Law 349") prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

124. Defendant is a business as defined by the statue.

125. Plaintiff and Class members are consumers as defined by the statute.

126. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of New York Gen. Bus. Law 349. The conduct alleged is a "business practice" as defined by the statute, and the deception occurred in New York state.

127. Defendant engaged in deceptive acts or practices in the conduct of business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a proximate and direct cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks in both its own and its third-party vendors' technology systems, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents involving other organizations, which was a direct and proximate cause of the Data Breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures at both its own and its third-party vendors' technology systems;

d. Failing to timely and adequately notify Plaintiff and Class members of the Data Breach;

e. Failing to oversee and monito third-party vendors responsible for the storage and transfer of PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, GLBA and any other applicable statutes.

128. Defendant's representations and omissions regarding data security were material because they were about the critical need and adequacy of Defendant's data security and ability to protect the confidentiality of PII.

129. Defendant acted intentionally and knowingly to violate New York's General Business Law, and recklessly disregarded Plaintiff's and Class members' rights.

130. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for

fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; and the other harms detailed herein.

131. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large. Defendant's violations of the statute have had an impact on the public, including the people of New York.

132. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and Class members that they could not reasonably avoid.

133. As such, Plaintiff and the Class members seek statutory damages in the maximum amount allowed per Class member, or, $50 for each of the more than 2.3 million victims of the Data Breach. Additionally, Plaintiff and the Class members seek injunctive relief necessary to enjoin further violations and recover costs of this action.

COUNT IV

UNJUST ENRICHMENT

134. Plaintiff repeats and re-alleges each and every allegation as if fully set forth herein.

135. This Count is pled in the alternative to the cause of action for Breach of Contract (Count II).

136. Plaintiff and Class members conferred a monetary benefit on Defendant by providing Defendant with their valuable PII.

137. Defendant enriched itself by saving the costs it reasonably should have expended on data security oversight and other measures to secure Plaintiff's and Class members' PII, which cost savings increased the profitability of the services.

138. Upon information and belief, instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security

obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

139. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

140. Defendant acquired the monetary benefit, PII, through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

141. Had Plaintiff and Class members known that Defendant had not adequately secured their PII, they would not have agreed to provide their PII to Defendant. Plaintiff and Class members have no adequate remedy at law.

142. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm.

143. Furthermore, as a direct and proximate result of Defendant's ineffective, unreasonable and inadequate data security practices, Plaintiff and Class members are at a current and ongoing imminent risk of identity theft and have sustained incidental and consequential damages, including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their PII; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their PII, which

remains in Defendant's and third-party control, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

144. Plaintiff and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

145. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

146. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid for Defendant's services.

COUNT V

DECLARATORY JUDGMENT

147. Plaintiff repeats and re-alleges each and every allegation as if fully set forth herein.

148. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state laws and regulations described in this Complaint.

149. Defendant owes a duty of care to Plaintiff and Class members, which required it to adequately secure and oversee the protection of Plaintiff and Class members' PII.

150. Defendant still possesses PII regarding Plaintiff and Class members.

151. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and Class members continue to suffer injury as a result of the compromise of their PII and the risk remains that further compromises of their PII will occur in the future.

152. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure its victims' PII and to timely notify victims of a data breach;

b. Defendant's existing data security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect PII; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure and oversee the protection of victims' PII.

153. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect victims' PII, including the following:

a. Order Defendant to provide a lifetime of credit monitoring and identity theft insurance to Plaintiff and Class members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

ii. ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

iii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. auditing, testing, and training its security personnel regarding any new or modified procedures;

v. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

vi. conducting regular database scanning and security checks;

vii. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

viii. meaningfully educating its users about the threats they face with regard to the security of their PII as well as the steps Defendant's customers should take to protect themselves.

154. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury and will lack adequate legal remedy to prevent another data breach. The risk of another such breach is real, immediate, and substantial. If another breach of Defendant's or third-party systems occurs, Plaintiff and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

155. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff and Class members will likely be subjected to

substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligations to employ such measures.

156. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendant, thus preventing future injury to Plaintiff and other customers whose PII would be further compromised.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on his own behalf and on behalf of all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action, appointing Plaintiff as the lead plaintiff in this Action, and appointing Plaintiff's below-listed counsel as lead counsel of this Action;

B. For an award of restitution, actual damages, compensatory damages, statutory damages, nominal damages and statutory penalties, in an amount to be determined, as allowable by law;

C. For an award of equitable and injunctive relief;

D. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiff and the Class which remains in Defendant's possession;

E. For an award of attorneys' fees and costs;

F. For pre- and post-judgment interest on any amounts awarded; and

G. For such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMAND

157. Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: August 7, 2023

Respectfully submitted,

/s/ *Israel David*

Israel David
Adam M. Harris
Blake Hunter Yagman
Madeline Sheffield
ISRAEL DAVID LLC
17 State Street, Suite 4010
New York, New York 10004
Tel.: 212-739-0622
Fax: 212-739-0628
Email: *israel.david@davidllc.com*
adam.harris@davidllc.com
blake.yagman@davidllc.com
madeline.sheffield@davidllc.com

Attorneys for Plaintiff Andre Lopez and the Class